



SPYWOLF

Security Audit Report



Completed on
July 3, 2023

@SPYWOLFNETWORK



@SPYWOLFNETWORK



SPYWOLF.CO





OVERVIEW

This audit has been prepared for **NudeCoin** to review the main aspects of the project to help investors make an informative decision during their research process.

You will find a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

“

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

”





TABLE OF CONTENTS

Project Description	01
Contract Information	02
Current Stats	03
Vulnerability Check	04
Threat Levels	05
Found Threats	06-A/06-C
Good Practices	07
Tokenomics	08
Team Information	09
Website Analysis	10
Social Media & Online Presence	11
About SPYWOLF	12
Disclaimer	13



NudeCoin



PROJECT DESCRIPTION

According to their whitepaper:

Introducing Nudecoin (\$NUDE), a disruptive force within the live cam space that is ready to revolutionize the adult entertainment industry.

Building upon a robust minimum viable product, we already boast hundreds of models across our dynamic platform, eagerly waiting for the implementation of our groundbreaking payment system. Our platform brings together a suite of features, including fan pages for personalized experiences, a tipping system that boosts earnings and engagement, messaging features for direct interaction, and most importantly, live cams for real-time entertainment.

Release Date: Presale starts in July, 2023

Category: Live cam



CONTRACT INFO

Token Name
NudeCoin

Symbol
NUDE

Contract Address
0x28FBa7Fe6d4CF1081b292d0226818378DcAabf6f

Network
Ethereum

Language
Solidity

Deployment Date
Jul 01, 2023

Verified?
Yes

Total Supply
169,696,969,696

Status
Not launched

TAXES

Buy Tax
none

Sell Tax
none

*Taxes can be changed in future



Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat



TOKEN TRANSFERS STATS

Transfer Count	3
Uniq Senders	2
Uniq Receivers	3
Total Amount	268439063029.78598 NUDE
Median Transfer Amount	87389366060.78601 NUDE
Average Transfer Amount	89479687676.59532 NUDE
First transfer date	2023-07-01
Last transfer date	2023-07-03
Days token transferred	3

SMART CONTRACT STATS

Calls Count	8
External calls	4
Internal calls	4
Transactions count	5
Uniq Callers	2
Days contract called	3
Last transaction time	2023-07-03 03:12:23 UTC
Created	2023-07-01 11:52:47 UTC
Create TX	0xbaf35a39ede5e5dc9a40d8a922d370ce63e47a6a7abaf7828974b099bf7f1e67
Creator	0x01f8c3a28ab259b8f7b9bb9705cdec15bec14285



VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed



THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.



FOUND THREATS

⚠ Medium Risk

Owner can change contract's auto swap settings.
If swapEnabled is true and swapThreshold is set to 0 and contract's token balances are 0, contract will halt on sell.

```
function setSwapEnabled(bool state) external onlyOwner {
    swapEnabled = state;
}

function setSwapThreshold(uint256 new_amount) external onlyOwner {
    swapThreshold = new_amount;
}

function _transfer(address sender, address recipient, uint256 amount) internal override {
    .....
    if (swapEnabled && !swapping && sender != pair) swapForFees();
    .....
}

function swapForFees() private inSwap {
    uint256 contractBalance = balanceOf(address(this));
    if (contractBalance >= swapThreshold) {
        swapTokensForETH(swapThreshold);
    }
}
```

- Recommendation:
 - Ensure that swapThreshold's value is always above 1 token (consider decimals)



Informational

Owner can set buy/sell fees up to 10%.

Combined buy+sell = 20%.

When fees are above 0, there will be certain amount of tokens that will be deducted from every transaction that users make.

Deducted amount will be as much as the fees % from total amount that user had bought, sold and/or transferred.

```
function SetFee(uint256 _totalTax, uint256 _totalSellTax) external onlyOwner{
    require (_totalTax <= 10, "Fee can't exceed 10%");
    require (_totalSellTax <= 10, "Fee can't exceed 10%");
    tBuyTax = _totalTax;
    tSellTax = _totalSellTax;
}
```

Owner can exclude address from fees.

When address is excluded from fees, the user will receive the whole amount of the bought, sold and/or transferred tokens.

```
function updateExcludedFromFees(address _address, bool state) external onlyOwner {
    excludedFromFees[_address] = state;
}
```



Informational

Any tokens can be withdrawn from the contract to the marketing wallet. When this function is present, in cases tokens sent into the contract by mistake or purposefully, marketing wallet can retrieve them.

```
function rescueERC20(address tokenAddress, uint256 amount) external {
    IERC20(tokenAddress).transfer(MarketingWallet, amount);
}

function rescueETH(uint256 weiAmount) external {
    payable(MarketingWallet).sendValue(weiAmount);
}
```

Owner can remove max transaction limit and max wallet limits. Current max transaction and max wallet limits are 2% of total supply.

```
uint256 public maxTransactionAmount = tsupply * 2/100;
uint256 public maxWalletAmount = tsupply * 2/100;

function removelimit() external onlyOwner{
    maxTransactionAmount = tsupply;
    maxWalletAmount = tsupply;
}
```



RECOMMENDATIONS FOR

GOOD PRACTICES

1

Consider fundamental tradeoffs

2

Be attentive to blockchain properties

3

Ensure careful rollouts

4

Keep contracts simple

5

Stay up to date and track development

NudeCoin

GOOD PRACTICES FOUND

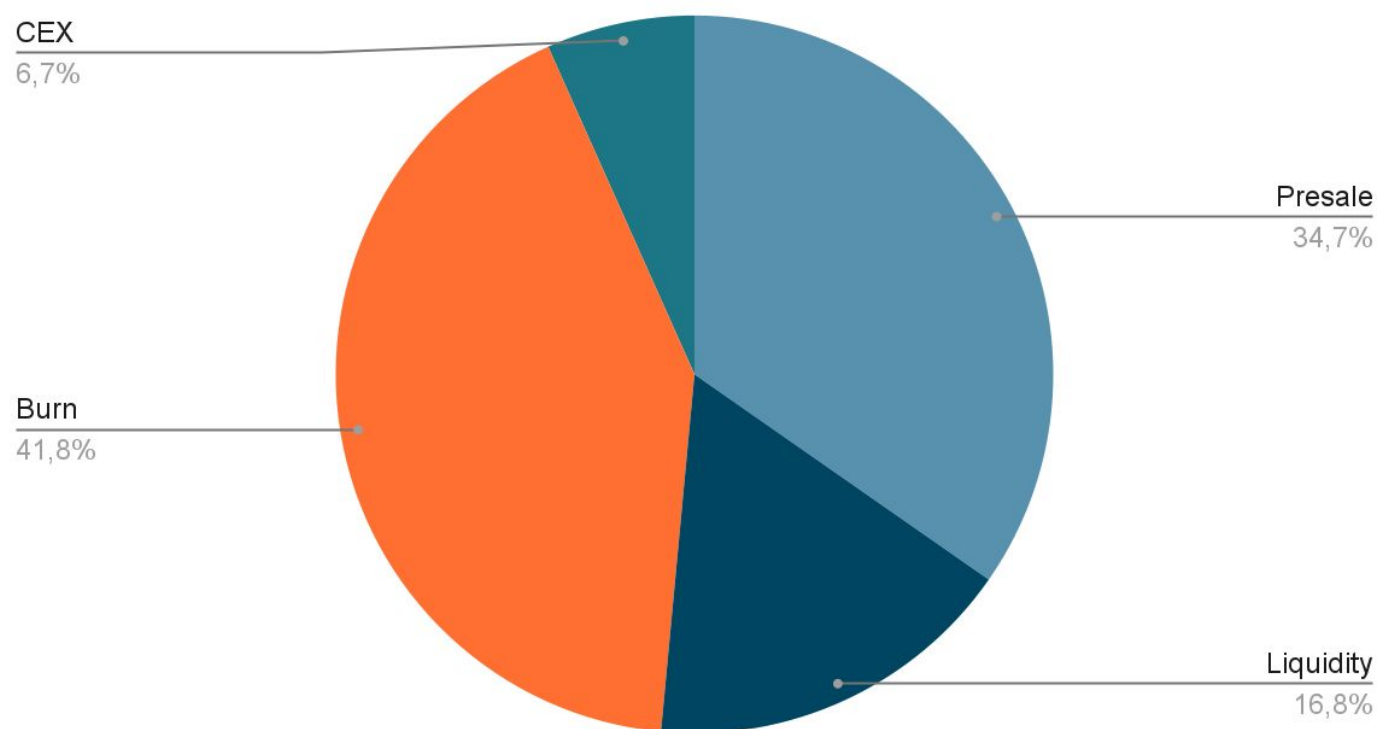
- ✓ The owner cannot mint new tokens after deployment
- ✓ The owner cannot set a transaction limit but only remove it. Current transaction limit is 2% of total supply



The following tokenomics are based on the project's whitepaper and/or website:

- 34.69% - Presale
- 16.8% - Liquidity
- 41.82% - Burn
- 6.69% - CEX

Tokens distribution



TOKENOMICS



THE TEAM

⚠ The team is anonymous

KYC INFORMATION

No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.





WEBSITE

Website URL

<https://nudecoin.bio/>

Domain Registry

<https://www.namecheap.com/>

Domain Expiration

2024-06-27

Technical SEO Test

Passed

Security Test

Passed. SSL certificate present

Design

Single page design with appropriate color scheme and graphics.

Content

The information helps new investors understand what the product does right away.

No grammar mistakes found.

Whitepaper

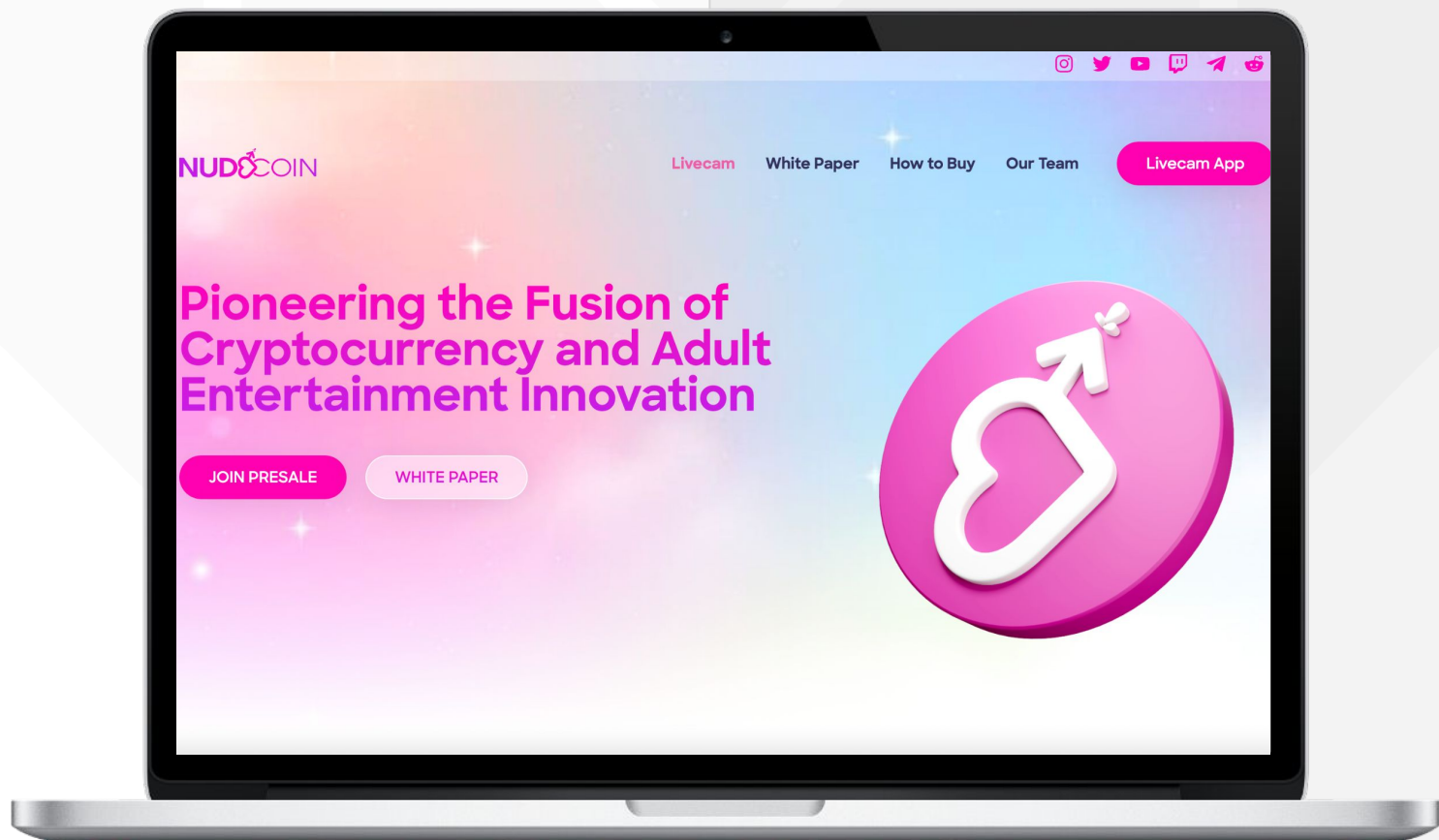
Well written, explanatory.

Roadmap

Yes, goals set with time frames.

Mobile-friendly?

Yes



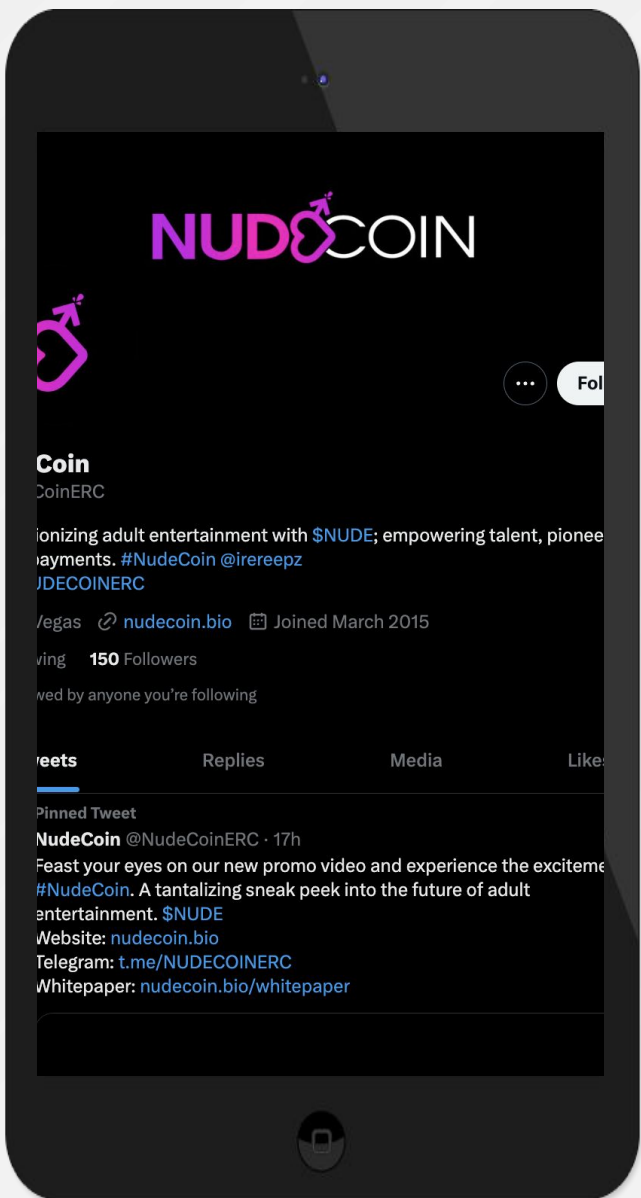
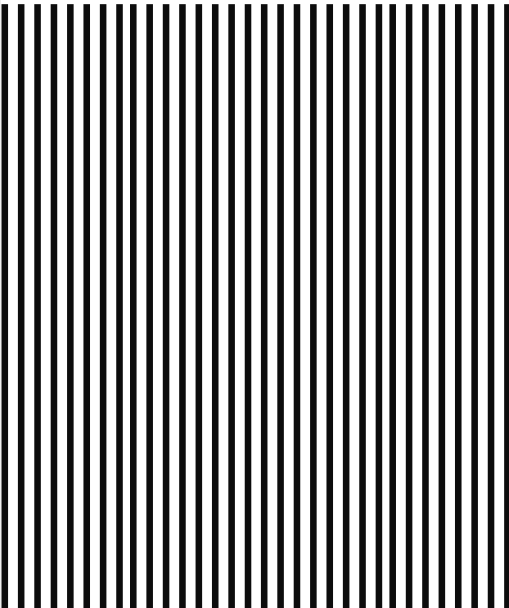
nudecoin.bio



SOCIAL MEDIA & ONLINE PRESENCE



ANALYSIS
Project's social media pages are active



Twitter
@NudeCoinERC

- 148 followers
- 2 total posts
- New account



Discord

- Not available



Telegram
@NUDECOINERC

- 453 members
- Active members
- Active mods



Medium

- Not available



SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 500 SUCCESSFUL CLIENTS
- ✓ MORE THAN 500 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE



[SPYWOLF.CO](https://spywolf.co)



[@SPYWOLFNETWORK](https://t.me/SPYWOLFNETWORK)



[@SPYWOLFNETWORK](https://twitter.com/SPYWOLFNETWORK)



Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.